Hans-Peter Königs

IT-Risikomanagement mit System

Praxisorientiertes Management von Informationssicherheits- und IT-Risiken

4. Auflage

Springer Vieweg

Edition <kes>

Herausgegeben von
P. Hohl, Ingelheim, Deutschland

Mit der allgegenwärtigen Computertechnik ist auch die Bedeutung der Sicherheit von Informationen und IT-Systemen immens gestiegen. Angesichts der komplexen Materie und des schnellen Fortschritts der Informationstechnik benötigen IT-Profis dazu fundiertes und gut aufbereitetes Wissen.

Die Buchreihe Edition <kes> liefert das notwendige Know-how, fördert das Risikobewusstsein und hilft bei der Entwicklung und Umsetzung von Lösungen zur Sicherheit von IT-Systemen und ihrer Umgebung.

Herausgeber der Reihe ist Peter Hohl. Er ist darüber hinaus Herausgeber der <kes>– Die Zeitschrift für Informations-Sicherheit (s.a. www.kes.info), die seit 1985 im SecuMedia Verlag erscheint. Die <kes> behandelt alle sicherheitsrelevanten Themen von Audits über Sicherheits-Policies bis hin zu Verschlüsselung und Zugangskontrolle. Außerdem liefert sie Informationen über neue Sicherheits-Hard- und -Software sowie die einschlägige Gesetzgebung zu Multimedia und Datenschutz.

IT-Notfallmanagement mit System
von Gerhard Klett, Klaus-Werner Schröder und Heinrich Kersten

Der IT Security Manager
von Heinrich Kersten, Gerhard Klett, und Klaus-Dieter Wolfenstetter

Information Security Risk Management
von Sebastian Klipper

IT-Sicherheit kompakt und verständlich
von Bernhard C. Witt

Konfliktmanagement für Sicherheitsprofis
von Sebastian Klipper

Praxis des IT-Rechts
von Horst Speichert

IT-Sicherheitsmanagement nach ISO 27001 und Grundschutz
von Heinrich Kersten, Jürgen Reuter und Klaus-Werner Schröder

Security Awareness
von Michael Helisch und Dietmar Pokoyski

Rollen und Berechtigungskonzepte
von Alexander Tsolkas und Klaus Schmidt

Hans-Peter Königs

IT-Risikomanagement mit System

Praxisorientiertes Management von Informationssicherheits- und IT-Risiken

4. Auflage

PRAXIS

Springer Vieweg

Hans-Peter Königs
Olsberg, Schweiz

ISBN 978-3-8348-1687-0 ISBN 978-3-8348-2165-2 (eBook)
DOI 10.1007/978-3-8348-2165-2

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Springer Vieweg

Gedruckt auf säurefreiem und chlorfrei gebleichtem Papier.

Springer Vieweg ist eine Marke von Springer DE. Springer DE ist Teil der Fachverlagsgruppe Springer Science+Business Media
www.springer-vieweg.de

Geleitwort

Die Unternehmenspraxis – insbesondere in der derzeitigen Euro-Krise – zeigt, wie eng die Chancen unserer Unternehmen mit Risiken aller Art verbunden sind. Aufgrund der Ereignisse in den letzten Jahren unternehmen die Gesetzgeber und Regulatoren immer neue Anläufe und Verbesserungen, um die Risiken sowohl für die Volkswirtschaft, als auch für das einzelne Unternehmen und letztlich den Bürger in einem erträglichen Mass zu halten.

Bei den wesentlichen Neuerungen denken wir beispielsweise an die Datenschutzgesetze, an die neuen Anforderungen des „Basler Ausschusses für Bankenaufsicht“ (Basel II und III) oder an die Anforderungen von Solvency II für Versicherungen. Solche und auch andere Vorgaben stellen nebst den Anforderungen an das Risikomanagement bzgl. der finanziellen Risiken auch jeweils Anforderungen hinsichtlich der Beherrschung der Informationssicherheits- und IT-Risiken.

Die Möglichkeiten der IT aufgrund der globalen Vernetzungen, die Anonymität von Angreifern im Internet sowie die Geschwindigkeit und Komplexität der Arbeitsprozesse und Systeme bieten neben den unbestreitbaren Chancen immer neue und leider auch grössere und schwer fassbare Risiken. Die Risikobeurteilung und -behandlung muss sich dabei an der Wesentlichkeit für die Erreichung der Geschäftsziele orientieren. Deshalb sind neben den Angriffspotentialen aus dem „Cyber Space“ auch Risiken, resultierend aus Verstössen gegen gültiges Recht, mangelhafte Verträge oder schlecht abgestimmtes und überwachtes Outsourcing zu berücksichtigen, um einige Beispiele zu nennen.

Das vorliegende Buch nimmt sich diesen aktuellen Anforderungen in einer für die praktische Umsetzung geeigneten Weise unter Berücksichtigung der aktuellen internationalen Standards an. So werden die unter dem Sammelbegriff „Management-Systeme“ die im Unternehmen zu integrierenden Unternehmensprozesse für das Risikomanagement (ISO 31000) wie auch für die Informationssicherheit (ISO/IEC 2700x-Reihe) und die Geschäftskontinuität (neuer Standard ISO 22301) behandelt.

Ein eigenes neues Kapitel ist dem „Cloud-Computing“ mit entsprechenden Lösungsansätzen für das Management der Risiken zugeschrieben. Die Mitarbeit des Autors in den relevanten Stan-

dardisierungs-Gremien der Schweizerischen Normenvereinigung lässt ihn aus einem reichen Fundus für die Entwicklung und den Einsatz solcher Standards schöpfen. Im Sinne einer ganzheitlichen Betrachtung der Leistung und Sicherheit der IT und der Informationen im Unternehmen geht das Buch auch auf das neue Rahmenwerk CobiT 5 ein.

Wie in den vorherigen Auflagen dieses Buches hat es der Autor wiederum sehr gut verstanden, die zum Teil komplexen Zusammenhänge in einer mit Beispielen und auf das Wesentliche beschränkten Darstellung anschaulich zu behandeln. Dabei kommen dem Autor zweifellos seine langjährigen didaktischen Erfahrungen aus seiner Tätigkeit als Dozierender für verschiedene Fächer des Risikomanagements an der Hochschule für Wirtschaft Luzern zugute.

Wir wünschen auch der vierten, in vielen Aspekten überarbeiteten und ergänzten Auflage den guten Erfolg der vorangegangenen Auflagen.

Dr. Thomas Siegenthaler, Präsident CSI Consulting AG

Vorwort zur 4. Auflage

Die Auflagen dieses Buches spiegeln den Kreislauf einer ständigen Anpassung an neue Gegebenheiten und einer kontinuierlichen Verbesserung wider. So hat sich seit der ersten Auflage im Jahr 2005 nicht nur die Risikolandschaft mit ihren Anforderungen, sondern, neben den gesetzlichen und regulativen Vorgaben, auch die Verfügbarkeit von Standards, Rahmen- und Regelwerken erheblich erweitert. Beispiele solcher Rahmen- und Regelwerke über Aspekte des Risikomanagements sind der ISO Standard 31000:2009 über Prinzipien und Richtlinien eines Risikomanagements, die zahlreichen ISO/IEC-Standards der 2700x-Reihe über Informationssicherheit, der internationale Standard ISO 22301:2012 über Geschäftskontinuität sowie die deutschen BSI-Standards 100-x oder die österreichischen Standards der Reihe ONR 4900x in diesen Themen. Erwähnenswert sind auch die neuerlichen Bemühungen zur Vereinheitlichung der ISO-Standards über Management-Systeme auf der Basis des neuen „ISO Guide 83".

Auch verwundert nicht, dass die Informationssicherheits-Risiken, beispielsweise bei der Verwendung von „Cloud-Computing" sowie bei der steigenden Ernsthaftigkeit von „Cyber-Threats", aber auch bei neuen gesetzgeberischen und regulatorischen Anforderungen in den letzten Jahren eine neue Relevanz erhalten haben. Die derzeit laufenden Standardisierungen, an denen ich in den relevanten Normen-Komitees der Schweizerischen Normenvereinigung mitarbeite, tragen solchen aktuellen Aspekten Rechnung. Doch ist es, trotz der starken Anlehnung an solche Standards, nicht Zweck dieses Buches, diese Standards zu interpretieren oder gar zu ersetzen. Vielmehr sollen für den Leser die wesentlichen praktischen Aspekte eines Risikomanagements aus der Sicht des Unternehmens sowie der IT und der Informationssicherheit herausgearbeitet werden. Somit ist das Buch Alternative und Ergänzung zu den heute vielfältig vorhandenen und in den Literaturhinweisen erwähnten Standardisierungs-Dokumenten. Selbstverständlich wird in dieser neuen Buchauflage die in den neueren Standards verwendete Terminologie des Risikomanagements, vor allem die des „ISO Guide 73:2009" angewandt.

Wie im erweiterten Titel des Buches erkennbar ist, beschränkt sich das Buch weder alleine auf die Risiken der Informationssi-

cherheit* noch alleine auf die Risiken der Informationstechnologie, sondern soll im Rahmen eines Unternehmens-Risikomanagements für beide Risiko-Felder Gültigkeit haben.

Somit verfolgt das Buch das Ziel, den derzeitigen Stand des Informationssicherheits-Risikomanagements und des IT-Risikomanagements in einer für den Anwender in der Praxis notwendigen Übersicht und Ausführlichkeit zu behandeln. Um dabei den Fokus eines „Leitfadens" nicht zu verlieren, wurden beispielsweise aufwändige quantitative Assessment-Methoden, welche hohe Anforderungen an das statistische Datenmaterial und an ihre praktische Umsetzung stellen, mit entsprechenden Hinweisen weniger umfassend und tief behandelt. Stattdessen wurden, insbesondere in den beiden ersten Buchteilen, die Möglichkeiten des Risiko-Assessments und der Risiko-Behandlung, wie sie für operationelle Risiken auf der Ebene des Gesamtunternehmens allenfalls in Betracht kommen, in den wesentlichen Grundzügen vorgestellt. Wie aktuelle Beispiele zeigen, können die Informationssicherheits-Risiken und IT-Risiken grosse Risiken für Unternehmen bedeuten. Man denke beispielsweise an den Ausfall wichtiger Produktionssysteme oder den Diebstahl geheimer Unternehmensdaten mittels Attacken über das Internet. Demzufolge bezweckt der Aufbau dieses Buches die Integration des Informationssicherheits-Managements und des IT-Risikomanagements in ein in das Führungssystem des Unternehmens integriertes Gesamt-Risikomanagement. So erweist sich die Strukturierung in die folgenden vier Buchteile als nützlich:

Teil A: Grundlagen erarbeiten

Teil B: Anforderungen aus Unternehmenssicht berücksichtigen

Teil C: Informations-Risiken erkennen und bewältigen

Teil D: Unternehmensprozesse meistern

Damit erklärt sich auch, dass in den ersten beiden Buchteilen die Grundlagen und die Anforderungen in einer für das Unternehmen allgemeinen Weise behandelt werden. Hingegen werden die für die IT- und Informations-Risiken spezifischen Inhalte im dritten Teil des Buches und die Umsetzung und die Integration des Informationssicherheits- und IT-Risikomanagements in die Unternehmensprozesse im vierten und letzten Teil des Buches behandelt.

* Sicherheit der Vertraulichkeit, Verfügbarkeit und Integrität von Informationen

Am Ende eines jeden Kapitels finden sich eine Zusammenfassung sowie einige Kontrollfragen und Aufgaben. Die Musterlösungen für die Kontrollfragen und Aufgaben können über den Online-Service im Internet abgerufen werden. Die URL dafür ist:

http://www.koenigs-media.ch/viewegbuch/

Fragen, fachliche Hinweise oder gar einen über den Online-Service möglichen Dialog sind mir herzlich willkommen.

Dank

Wie die neuen Auflagen des Buches unterliegen auch die Ausbildungsgänge zum „Bachelor of Information Security“ und zum „Master of applied Studies in Information Security“ an der Hochschule Luzern, wo ich neben meiner Beratertätigkeit als Dozierender für Risikomanagement tätig bin, einem kontinuierlichen Verbesserungsprozess. Für die aus dieser Tätigkeit erhaltenen wertvollen Anregungen meiner Studierenden und Dozenten-Kollegen möchte ich mich an dieser Stelle herzlich bedanken.

Für die vielen Diskussionen und wertvollen Ratschläge zu den Erweiterungen in der vierten Auflage danke ich meinem langjährigen Berufskollegen Domenico Salvati und meinem Beraterkollegen Daniel Farner der Firma CSI Consulting AG für die stete Bereitschaft, einzelne Themen und deren Praxistauglichkeit zu diskutieren. Mein Dank gilt auch dem Lektorat des Springer Vieweg-Verlags für seine Unterstützung und seine wertvollen Hinweise.

Mein besonderer Dank geht an meine Tochter Nicole Königs Balfry für das sorgfältige Korrekturlesen sowie an meine Frau Diemuth Königs, Autorin historischer Bücher, die mir in allen Belangen mit Rat und Tat zur Seite steht.

Olsberg im September 2012 Hans-Peter Königs

Inhaltsverzeichnis

1 Einführung

„Erstens kommt es anders und zweitens als man denkt“. Dieses von Wilhelm Busch geprägte Prinzip wird im vorliegenden Buch nicht widerlegt. Doch warum beschäftigen wir uns denn überhaupt mit Risiken? Diese Frage und wie wir uns mit den Risiken im Allgemeinen und mit den Informationssicherheits- und den IT-Risiken im Unternehmen im Besonderen auseinandersetzen können, sollte spätestens nach dem Lesen dieses Buches beantwortet werden können.

1.1 Warum beschäftigen wir uns mit Risiken?

Unsere tagtäglichen Erfahrungen zeigen an einfachen Beispielen, dass wir mit geeigneten Vorkehrungen und Massnahmen das Auftreten von negativen Ereignissen oder auch die Konsequenzen solcher Ereignisse vermindern können. Wem es je passiert ist, dass kurz vor der Fertigstellung einer umfangreichen Schreibarbeit am PC die Informationen unwiederbringlich gelöscht waren, wird die Nützlichkeit einer regelmässigen Informationensicherung auf ein anderes Speicher-Medium kaum in Frage stellen.

Häufigkeiten reduzieren oder negative Konsequenzen mildern

Negative Ereignisse (z.B. Unfälle) können mit noch so weiser Voraussicht und entsprechenden Massnahmen nie gänzlich vermieden werden. Doch können mit entsprechenden Vorkehrungen entweder die Häufigkeiten solcher Ereignisse reduziert oder ihre negativen Konsequenzen gemildert werden.

Das am 11. März 2011 stattgefundene Erdbeben in Japan und die nachfolgende Tsunami- und Atomreaktor-Katastrophe haben uns in eklatanter Weise vor Augen geführt, wie den Verhältnissen angemessene vorsorgliche Massnahmen den Tsunami zwar nicht hätten verhindern, aber die Auswirkungen – vor allem die nachfolgende Reaktorkatastrophe – wesentlich hätten reduzieren können. So kam auch der am 5. Juli 2012 veröffentlichten Bericht einer eingesetzten parlamentarischen Untersuchungskommission zum Schluss, dass die „von Menschen verursachte Katastrophe“ der Kernschmelze „vermeidbar“ gewesen wäre.

H.-P. Königs, *IT-Risikomanagement mit System*, Edition <kes>,
DOI 10.1007/978-3-8348-2165-2_1, © Springer Fachmedien Wiesbaden 2013

Auch denken wir sofort an mögliche Unterlassungen, wenn wir, wie am 15. Januar 2009, lesen: „Die elektronischen Fahrpläne und das Buchungssystem der Deutschen Bahn waren in ganz Deutschland stundenlang ausgefallen. Der Computerausfall hatte am Mittwoch bundesweit zu Verspätungen im Bahnverkehr geführt."

Ähnliches, aber in umgekehrter Richtung, gilt für die positiven Ereignisse, die wir selbstverständlich herbeiwünschen und für die wir uns einen möglichst positiven Effekt erhoffen. Solche ungewissen wünschbaren positiven Ereignisse bezeichnen wir als Chancen.

Für solche Ereignisse ergreifen wir Massnahmen, um den positiven Effekt mit grösstmöglicher Wahrscheinlichkeit oder mit möglichst günstigen Ergebnissen herbeizuführen. So soll beispielsweise die Fernsehwerbung für ein Kosmetikprodukt dafür sorgen, dass das Produkt möglichst häufig gekauft wird. Oder ein Softwareprodukt wird so angeboten, dass es zum einen möglichst häufig gekauft wird und zum anderen einen möglichst hohen Preis erzielt.

Risiken und Chancen

Sowohl für die Risiken als auch die Chancen gibt es Massnahmen, die das gewünschte Resultat besser oder schlechter herbeiführen können. Ein zentraler Aspekt des Umgangs mit Risiken und Chancen ist, unter den massgeblichen Bedingungen, die optimal geeigneten Massnahmen herauszufinden und zu realisieren.

Die eben skizzierte Beschäftigung mit Risiken ist grob vereinfacht das, was wir unter „Risikomanagement" verstehen. Um mit allen und zum Teil hoch abstrakten Aspekten zu den gewünschten optimalen Ergebnissen zu kommen, braucht es ein grosses Mass an Systematik. Gerade wenn es um hohe Risiken und hohe Massnahmenkosten geht, die den Unternehmen durch die Informations-Technologie entstehen, ist es wichtig, diese ganzheitlich, systematisch und transparent zu behandeln.

„Risikomanagement" mit systemischen Modellen

Die dafür in diesem Buch verwendeten Modelle sind als „systemische" Modelle zu verstehen. Dabei kann eine Risiko-Ursache verschiedene Auswirkungen und eine Auswirkung verschiedene Ursachen haben. Um die meist „komplexe" Wirklichkeit möglichst gut zu modellieren, enthalten daher die Problemlösungs-Prozesse des Risikomanagements entsprechende Rückkopplungen und Iterationen ([Ulri91], S. 114). Mit diesem „systemischen" Ansatz findet auch der Titel dieses Buches „IT-Risikomanagement mit System" seine Erklärung.

1.2 Risiken bei unternehmerischen Tätigkeiten

Risiken und Chancen sind in jedem Unternehmen – wenn auch nicht immer offensichtlich – vorhanden. Es gilt der Grundsatz, dass mit dem Ergreifen von Chancen auch immer Risiken eingegangen werden müssen. Dabei ist es eine normale menschliche Eigenschaft, die Risiken aus dem Bewusstsein zu verdrängen. Dennoch ist der sorgfältige Umgang mit Risiken, gleichermassen wie das Wahrnehmen von Chancen, eine der wichtigsten unternehmerischen Verantwortlichkeiten und muss in der Unternehmens-Politik, in der Unternehmens-Strategie sowie in allen unternehmerischen Handlungen gepflegt werden. Ist es doch das Wohl des Unternehmens und gar sein Überleben, das vom richtigen Umgang mit den Risiken abhängig ist.

Leidtragende

Die Leidtragenden der Risiken sind auch nicht alleine die Eigentümer des Unternehmens, sondern alle an einem Unternehmen beteiligten Kreise, die sog. Anspruchsgruppen (Stakeholders), wie Beschäftigte, Kapitalgeber, Verbände, Partner, Lieferanten, Behörden, Kommunen und der Staat. So haben die in den letzten Jahren aufgetretenen Schadensereignisse bewirkt, dass das Risikomanagement in den meisten Industriestaaten zu einer vom Gesetzgeber verordneten „Muss-Disziplin" der Unternehmensführung geworden ist.

1.3 Inhalt und Aufbau dieses Buchs

Die unterschiedlichen Risiken in einem Unternehmen sind in ihrer Art und Entstehung stark voneinander abhängig und tragen letztendlich zum Erfolg oder Misserfolg eines Unternehmens in entscheidendem Masse bei. Deshalb muss die Steuerung und Überwachung der Risiken bereits auf der obersten Ebene der Unternehmensführung erfolgen. Das Buch behandelt zwar speziell die Informationssicherheits- und IT-Risiken, dennoch müssen die Bedrohungen, Massnahmen und Prozesse zum Management dieser Risiken in einem ganzheitlichen Zusammenhang zur Unternehmenssicht und dessen Zielen, Anforderungen und Management-Prozessen gesehen werden. Demzufolge wird vor der detaillierten Behandlung der Informationssicherheits- und IT-Risiken im Teil C des Buches der dazu notwendige Vorspann in den Teilen A und B behandelt.

Teil A: Grundlagen erarbeiten

Somit werden in **Teil A** des Buches die für ein ganzheitliches Risikomanagement in einem Unternehmen allgemeinen Grundlagen und Instrumente aufgezeigt.

Teil B: Anforderungen aus Unternehmenssicht berücksichtigen

Im Teil B werden die an das Unternehmen gestellten heute aktuellen Anforderungen an ein Risikomanagement und die Voraussetzungen und Prozesse für die in die Management-Prozesse des Unternehmens integrierten Risiko-Aspekte beleuchtet. Die dazu zusammengestellten Konzepte, Methoden und Instrumente haben zum Ziel, ein möglichst effektives Risikomanagement mit vertretbarem Aufwand aufzubauen und zu betreiben.

Teil C: Informations-Risiken erkennen und bewältigen

Im Teil C werden die Risiken der Informationen und der Informationstechnologie detailliert behandelt und entsprechende Methoden und Verfahren speziell zum Management der Informationssicherheit- und IT-Risiken beschrieben. Der gebräuchliche aber unscharfe Begriff der „Informations-Risiken" schliesst dabei die Informationssicherheits-Risiken wie die Risiken im Zusammenhang mit der Leistungserbringung der Informatik ein.

Teil D: Unternehmensprozesse meistern

Im Teil D wird sodann gezeigt, wie sich die verschiedenen Risiken, darunter die operationellen Risiken der Informationssicherheit und der Informations-Technologie, in einen gesamten Risikomanagement-Prozess des Unternehmens einfügen lassen und wie unternehmenswichtige Risikomanagement-Prozesse wie die Geschäftskontinuitäts-Planung im Risikomanagement-Prozess verankert werden können.

Teil A

Grundlagen erarbeiten

2 Elemente für die Durchführung eines Risikomanagements

Akzeptable Restrisiken

Die Beschäftigung mit den Risiken dient vor allem ihrer Erkennung und Bewertung sowie der Erarbeitung von Massnahmen und deren Umsetzung. Durch die Massnahmen sollen die Risiken auf akzeptable „Restrisiken" reduziert werden.

Risikomanagement

Auf der Basis von Art, Quantität und Qualität der Risiken sowie einiger weiterer Kriterien sollen möglichst optimale Massnahmen-Lösungen gefunden und umgesetzt werden, aber auch akzeptable Restrisiken toleriert und ohne weitere Behandlung bewusst getragen werden können. Die koordinierten Aktivitäten zur Steuerung von Risiken im Unternehmen werden als „Risikomanagement" bezeichnet. Die in Abbildung 2.1 gezeigten hauptsächlichen Aktivitäten eines Risikomanagements werden vorteilhaft in einer prozessorientierten Weise durchgeführt.

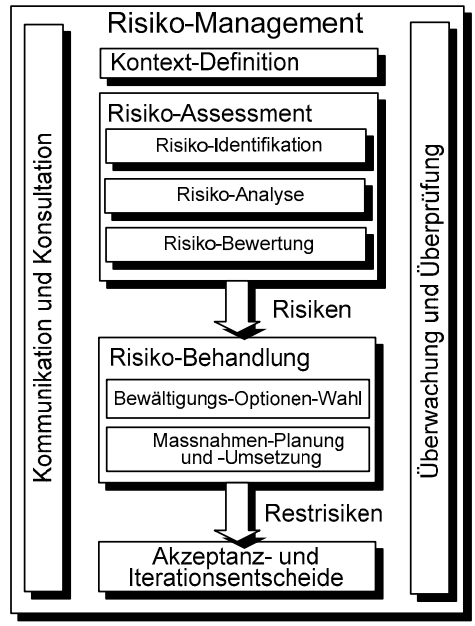

Abbildung 2.1: Aktivitäten für das Risikomanagement

H.-P. Königs, *IT-Risikomanagement mit System*, Edition <kes>,
DOI 10.1007/978-3-8348-2165-2_2, © Springer Fachmedien Wiesbaden 2013

Das „Risikomanagement“, wie es in diesem Buch sowohl generell aus Unternehmenssicht als auch spezifisch für die Gebiete der Informationssicherheit und der Informationstechnologie behandelt wird, ist eine wichtige Teil-Disziplin der Unternehmensführung.

Interdisziplinäre Vernetzung Risikomanagement

Eine solche Anwendung des Risikomanagements hat zudem einen hohen interdisziplinären Stellenwert, können doch beispielsweise die „Informationssicherheits-Risiken“ grosse andere Risiken in der Volkswirtschaft, im Gesundheitswesen, im Kommunikations-, Energie-, Verkehrs- und Transportwesen sowie ganz allgemein in der Gesellschaft nach sich ziehen. Beispiele: Datendiebstahl bei Sony von Namen, Passwörtern und Kreditkartennummern, undurchschaubare Funktionen bei sozialen Netzwerken, Cyber-Attacken mit Trojanern, mit denen Kriminelle die Computer von Privatpersonen und Unternehmen zu Betrugszwecken ausspionieren bis hin zu Staats- und Wirtschaftsspionage und dem heute zur Realität gewordenen „Cyber-Krieg“.

Terminologie und Standards

Die im Zusammenhang mit „Risikomanagement“ in den einzelnen Disziplinen verwendete Terminologie ist vielfältig und teilweise noch uneinheitlich. Auf diesem Hintergrund sind die Standardisierungen einer Terminologie im ISO Guide 73 [Isog09] sowie die Standards ISO 31000:2009 [Isor09] und ISO/IEC 27005:2011 [Isoi11] oder des US-amerikanischen „Committee of Sponsoring Organizations of the Treadway Commission“ [Cose04] als sehr begrüssenswert anzusehen. Doch weisen solche Standards, trotz der Harmonisierungsbestrebungen durch die ISO, im näheren Detail immer noch Unterschiede auf, die wahrscheinlich, aufgrund der spezifischen Anforderungen für einen bestimmten Kontext und der nationalen Präferenzen bei den Abstimmungen, nie vollständig harmonisiert werden können. Die Standards über Risikomanagement haben somit meist lediglich Empfehlungscharakter. Dieses Buch orientiert sich bezüglich Risikomanagement, wo immer angezeigt, an der im ISO Guide 73:2009 festgelegten Terminologie und den darauf abgestimmten „generischen“ Grundsätzen und Richtlinien des Standards ISO 31000:2009. Doch in einigen wichtigen Details finden auch Ergänzungen aus der Praxis des Autors sowie anderen Standards wie der Österreichischen Standardreihe ONR 49000:2008 ff (vgl. [Onri08]) oder des Standards ISO/IEC 27005:2011 über ein „Information Security Risk Management“ Verwendung.

2.1 Fokus und Kontext Risikomanagement

Fokussierung auf Betroffene

Die aus dem Risikomanagement resultierenden Massnahmen bezwecken, die Gefahrensituationen oder die Folgen von Schadensereignissen für die „Betroffenen“ zu beseitigen oder zu vermindern.

Je nachdem wie die Aufgabenstellung für das durchzuführende Risikomanagement lautet, können die Betroffenen, Einzelpersonen, Gruppen von Personen oder auch, wie in diesem Buch, Unternehmen sein. Die Risiken, die wir im Rahmen dieses Buches betrachten, fallen bei einzelnen Produkten oder Dienstleistungen, bei einzelnen Organisationseinheiten oder auf der Ebene des Gesamtunternehmens an.

Neben der Fokussierung auf die Betroffenen ist die Bezeichnung und Abgrenzung der Gegenstände* für die möglichen Schadensereignisse nötig. Auch das Umfeld der betrachteten Gegenstände bedarf der Definition und Abgrenzung. Diese Definitionen und Abgrenzungen sind aus den Blickwinkeln der Gefahrensituationen, der an der Risikobeurteilung und Behandlung beteiligten Stellen sowie der massgeblichen funktionalen Zusammenhängen notwendig.

Massgeblicher Kontext

Bereits zu Beginn einer Risikomanagement-Aufgabe ist die Fokussierung und die Bestimmung des massgeblichen Kontextes unabdingbare Voraussetzung. Mehr über die Inhalte des „Kontexts“ sowie die Aktivitäten bei den einzelnen Management-Aktivitäten sind im Kapitel 3 dargelegt.

2.2 Definition des Begriffs „Risiko“

Im Hinblick auf eine möglichst breite Anwendung lautet die ISO-Definition ISO/IEC Guide 73:2009 [Isov09]:

> Risiko ist die Auswirkung von Unsicherheit auf Ziele.

Diese grobe Definition, schliesst zwar objektive und subjektive Betrachtungen mit ein, ist aber in der Praxis nicht allzu hilfreich.

---

* Der Begriff „Gegenstand“ wird in diesem Buch synonym zu „Objekt“ sowohl für greifbare als auch für abstrakte Güter, Objekte und Strukturen verwendet und schliesst den in der englischsprachigen Standardisierung oft verwendeten Begriff „Asset“ ein.

In der Praxis sind deshalb je nach Anwendungsgebiet aussagekräftigere Definitionen anzutreffen*.

So werden für betriebswirtschaftliche Fragestellungen, wie sie in diesem Buch vorkommen, Verluste oder Schäden als die negativen Folgen von „**Zielabweichungen**“ eines vorgängig definierten Ziels verstanden. Mit den ursächlichen Bedrohungen, welche Schäden mit einer gewissen Häufigkeit hervorrufen können, ergibt sich folgende für den Praxiseinsatz sinnvolle Risiko-Definition (vgl. [Brüh01]):

Risiko-Definition

> Risiko ist eine nach Wahrscheinlichkeit (Häufigkeit) und Auswirkung bewertete Bedrohung eines zielorientierten Systems†. Das Risiko betrachtet dabei stets die negative, unerwünschte und ungeplante Abweichung von System-Zielen und deren Folgen.

Risiko / Chance

Dem Risiko steht meist eine Chance gegenüber, welche ein positives Ergebnis in Aussicht stellt. Bei den in diesem Buch betrachteten „Operationellen Risiken“ besteht jedoch meist keine unmittelbare Verknüpfung des Risikos mit einer Ertragsquelle. Daher lassen sich die Risiken und die dazugehörige Chancen solcher Risiken meist auch nicht mit dem gleichen Lösungsansatz behandeln, was das Abwägen der Risiken mit den Chancen entsprechend schwierig gestaltet.

Die obige Risiko-Definition lässt ein breites Anwendungsspektrum zu. So können die mit Unsicherheit behafteten Ziele in der Form elementarer Eigenschaften, aber auch in der Form komplexer qualitativer oder quantitativer Anforderungen formuliert werden. Von der Zieldefinition hängt es primär ab, was als Abweichung vom Ziel und deren Folgen (Konsequenzen) und damit als Risiko erklärt werden kann. So bestehen auch zur Ana-

---

* In einer der fünf Fussnoten zum Begriff Risiko bemerkt der ISO/IEC Guide 73:2009 [Isov09] beispielsweise, dass Risiko oft als „Kombination von Likelihood eines Ereignisses und seiner Konsequenzen“ ausgedrückt wird.

† Unter System wird in diesem Zusammenhang ein allgemeines System verstanden, das beispielsweise ein ökonomisches, ein gesellschaftliches oder ein technisches System mit zielorientierten Werten sein kann. Systeme mit ihren Subsystemen interagieren untereinander und werden für eine Risikobetrachtung entsprechend definiert und abgegrenzt.

lyse und Bewertung der Abweichungen von Zielen vielzählige Möglichkeiten, z.B. in der Form technischer Risikoaussagen, wie Mass über Anzahl und Ausmass von technischen Fehlern oder in der Form stochastischer Risikomassen in zeit- und geldwerter Skalierung oder gar in der Form von Indikatoren (s. Abschnitte 2.8 und 2.8.2).

Folgen der Ziel-Abweichungen

Wird die obige Risiko-Definition beispielsweise auf Projektrisiken angewendet, dann sind hauptsächlich die Folgen der Ziel-Abweichungen bezüglich „Dauer“, „Budget“ und „Qualität“ zu betrachten. Wenden wir die oben angegebene Definition auf Informationen und IT-Gegenstände an, dann resultieren die Sicherheits-Risiken und deren Folgen aus Abweichungen von den elementaren System-Zielen, „Vertraulichkeit“, „Integrität“ und „Verfügbarkeit“. Benützen wir die obige Definition bezüglich der Einhaltung einer gesetzlichen Vorschrift, dann könnte die aus einer Abweichung (Nichteinhaltung) resultierende Konsequenz beispielsweise der Verlust einer Banklizenz mit den entsprechenden Vermögensverlusten bedeuten. Solche auf der Erfüllung komplexer Anforderungen beruhenden Risiken werden oft unter dem Begriff „Compliance-Risiken“ zusammengefasst.

Unerwünschte Zielabweichungen

Die „unerwünschten Ziel-Abweichungen“ können eintreten, wenn entsprechende Bedrohungen vorhanden sind. So kann beispielsweise die Bedrohung „Krankheit Mitarbeiter“ eine negative Abweichung vom Ziel: „Fertigstellungs-Termin“ eines Projekts bewirken.

Bedrohungen

Eine Bedrohung wirkt sich umso häufiger und stärker aus, als geeignete Massnahmen fehlen. Eine geeignete Massnahme im gerade gegebenen Beispiel wäre, den krank gewordenen Mitarbeiter kurzfristig durch eine andere gleichermassen geeignete Person ersetzen zu können. Ist eine solche Massnahme nicht vorhanden, sprechen wir von einer Schwäche, Verletzlichkeit oder Schwachstelle des Systems.

Schwäche / Schwachstelle / Verletzlichkeit

Wahrscheinlichkeit von möglichen Folgen

Aus den Bedrohungen und den Schwächen des Systems ergibt sich die Wahrscheinlichkeit, mit der eine Abweichung vom gesetzten Ziel mit bestimmten negativen Folgen eintritt. Eine solche Abweichung kann plötzlich, aber auch schleichend oder intermittierend, d.h. mit einer gewissen Zeitabhängigkeit, eintreten. Als Beispiel einer zeitabhängig eintretenden Abweichung vom Ziel „Vertraulichkeit der Daten“, könnte ein über längere Zeit unentdeckt wiederholter Datendiebstahl genannt werden.

Die Folgen (Konsequenzen)* der Abweichungen vom Ziel bezeichnen wir als Schaden (auch Tragweite oder Verlust).

Folgen einer Ziel-Abweichung

So kann die Abweichung von einem geplanten Projekttermin finanzielle Einbussen zur Folge haben und/oder das Ansehen der Firma auf dem Markt beeinträchtigen (Reputations-Schaden). Die Folgen einer Ziel-Abweichung, wie die Abweichung selbst, können entweder ein zeitunabhängiges oder ein mit der Zeit veränderliches Ausmass aufweisen. So bedürfen die Ereignisse mit zeitlich anwachsendem Ausmass, z.B. Brandschäden, auch einer der Schadensentwicklung entsprechenden Risikobewältigung.

Keine Möglichkeiten von Zielabweichungen = „sicher"

Bestehen hingegen keine Möglichkeiten von Ziel-Abweichungen, so resultiert definitionsgemäss auch kein Schaden, wir sind also „sicher".

Bei bestimmten Zielen (z.B. Fertigstellungstermin in einem Projekt) kann eine Zielabweichung durchaus auch positive Folgen aufweisen. In diesem Falle haben wir es definitionsgemäss mit einer Chance zu tun. Bei den Massnahmenentscheidungen zur Bewältigung eines Risikos sind die möglichen Chancen ebenfalls in geeigneter Weise zu berücksichtigen.†

„System-Ziel" / „Sicherheits-Ziel"

Da wir die Vorgänge um ein Risiko systemisch betrachten (Ursachen, Auswirkungen etc.), verwenden wir für diese Art von Zielen den Begriff „System-Ziel". In der Informationssicherheit wird statt System-Ziel oft auch der Begriff „Sicherheits-Ziel" verwendet.

Risiko-Ziel

Ein System-Ziel bei der Risikobestimmung ist wiederum nicht zu verwechseln mit einem „Risiko-Ziel", bei dem es um eine Vorgabe geht, eine bestimmte Risikohöhe nicht zu überschreiten. Risiko-Ziele werden oft auch in der Form von akzeptierbaren „Risiko-Toleranzen" ausgedrückt.

---

* Die Auswirkung eines Ereignisses wird auch als „Impact" bezeichnet. Die gesamthaften Konsequenzen können aus mehreren Impacts resultieren. Die negativen Konsequenzen eines Ereignisses bezeichnen wir in diesem Buch als Schaden oder Verlust.

† Die Analyse von Chancen sowie die Massnahmen zur deren Realisierung werden im Rahmen dieses Buches über Informationssicherheits- und IT-Risikomanagement nicht speziell behandelt.

Beispiel:

Es besteht das Ziel, das Produktionssystems „FabriStock“ am 1. November 2012 in Betrieb nehmen zu können. Das System-Ziel heisst somit „Einhaltung des Einführungstermins“. Hingegen könnte ein mögliches Risiko-Ziel heissen: Die Kostenfolge durch eine Terminabweichung, multipliziert mit der Wahrscheinlichkeit ihres Auftretens, darf nicht mehr als 20’ 000 € betragen (=Risiko). Bei einem Risiko von 10’ 000 € ist das Risiko-Ziel noch bestens eingehalten, wir befinden uns sozusagen noch im „grünen Bereich“. Das Beispiel zeigt, dass erst mit der Einführung eines „Risiko-Ziels“ die Nichteinhaltung eines System-Ziels relativiert werden kann. Wir sehen später, dass wir diese Relativierung mit der Aufgabe „Risiko-Bewertung“ (risk evaluation) durchführen.

2.3 Risiko kombiniert aus Wahrscheinlichkeit und Konsequenz

Die oben angeführten verbalen Definitionen des Risikos liefern noch keine „messbaren“ Ergebnisse. Messbare Ergebnisse sind aber für viele Massnahmen-Entscheide oder für die Vergleichbarkeit von Risiken untereinander und mit anderen Risiken wichtig.

Eine einfache Möglichkeit, das Risiko messbar auszudrücken, besteht gemäss der untenstehenden Formel in der Multiplikation von Wahrscheinlichkeit und Schadensausmass. Es gilt jedoch vorweg zu bemerken, wie im Abschnitt 2.4 noch näher erläutert, dass solche Berechnungen problematisch sind und nur unter bestimmten Bedingungen zielführend sein können.

$$\mathbf{R = p_E \times S_E}$$

R: Risiko;
p_E: Wahrscheinlichkeit, dass ein Schadensereignis mit dem Schaden S_E eintritt;
S_E: Ausmass des Schadensereignisses (auch Tragweite oder Verlust).

Anstelle der „theoretischen Wahrscheinlichkeit“ p_E wird meist die empirisch bestimmbare „relative Häufigkeit“ H_E des Schadeneintritts eingesetzt.

Eine solche Formel zeigt zwar rudimentär, dass das Risiko grösser wird, wenn die Wahrscheinlichkeit (relative Häufigkeit) eines